Navn: _____ Dato: _____ Poeng: _____

Slik skjuler du IP-adressen din Arbeidsark

Skjuling av IP-adresser, maskering av posisjon, proxy, Tor og forebygging av DNS- og WebRTC-lekkasjer

OPPLÆRINGSOVERSIKT FOR VPN

ELEV
STUDENTSTATUS
Spor for nettverksforsvarere

SIKKER
TILKOBLINGSSTATUS
Beskytte datapakker

AKTIV
LEKKASJEBESKYTTELSE
DNS- og IPv6-lekkasjebeskyttelse

Velkommen! Dette aktivitetsheftet veileder deg gjennom de grunnleggende prinsippene i virtuelle private nettverk (VPN-er). Du utforsker hvordan krypterte tunneler sikrer dataene dine, hvordan nettverksprotokoller fungerer, og hvordan du identifiserer og begrenser personvernlekkasjer.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk VPN-begreper og -protokoller.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms VPN-veiledning

URL: https://www.vpn.com/no/vpn/

Din læringsveiledning for VPN

- Forklar hvordan IP-adresser fungerer, og hvordan de avslører lokasjoner.
- Sammenlign proxyer, Tor og VPN-er for å skjule nettverksadresser.
- Identifiser metoder for å oppdage og forhindre DNS- og WebRTC-lekkasjer.
- Forstå hvordan nettsteder sporer brukere gjennom den offentlige IP-adressen deres.
- Vurder multi-hop-ruting og krypterte tunneler for IP-beskyttelse.

INSTRUKSJONER FOR ARBEIDSARK OM IP-BESKYTTELSE

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på skjuling av IP-adressen din og forebygging av lekkasjer. Avslutt med bonusaktiviteten Tenk raskt.

SKJUL IP-ADRESSEN DIN (INNLEDNING)

IP-adressen din er som en digital postadresse som avslører hvor du fysisk befinner deg og hvilke nettvaner du har. Å skjule IP-adressen er det første forsvaret mot sporing på nett, profilering og geografiske sperrer. Når du forstår hvordan du maskerer adressen din på en trygg måte, hjelper det deg å beskytte personvernet ditt på nettet.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva avslører en enhets offentlige IP-adresse for nettstedene du besøker?

- A. Brukerens kredittkortnummer
- B. Din omtrentlige plassering og navnet på internettleverandøren din
- C. Hele den lokale filkatalogen
- D. Innstillingene for tastaturspråk

2. Hvilken metode skjuler IP-adressen din og krypterer all trafikk på hele systemet?

- A. En vanlig nettproxy
- B. Å tømme informasjonskapslene i nettleseren
- C. Et virtuelt privat nettverk (VPN)
- D. Å deaktivere din egen innebygde brannmur

3. Hva er en stor personvernbegrensning ved å bruke en gratis webproxy?

- A. Den krypterer ikke datatrafikk på offentlige nettverk
- B. Den krever installasjon av et eksternt operativsystem
- C. Den er helt ulovlig i USA
- D. Den krever en dedikert telefonlinjetilkobling

4. Hvordan gir Tor-nettverket brukerne høy anonymitet?

- A. Ved å øke tilkoblingshastigheten
- B. Ved å rute trafikken gjennom tre reléer drevet av frivillige
- C. Ved å registrere navnet ditt i en global database
- D. Ved å begrense tilgangen til bare offentlige etater

5. Hva er en DNS-lekkasje?

- A. En feil ved sending av e-post til feil adresse
- B. Når DNS-forespørsler omgår VPN-tunnelen og går til internettleverandøren
- C. En maskinvarefeil i strømforsyningen til den lokale ruteren
- D. En oppdatering av driveren til det lokale nettverkskortet

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. En proxyserver krypterer operativsystemets bakgrunnstrafikk akkurat som en VPN.

- ○ Sant
- ○ Usant

7 Spørsmål 7

7. Tor-ruting er svært sikker, men reduserer nettlesehastigheten.

- ○ Sant
- ○ Usant

8 Spørsmål 8

8. WebRTC-lekkasjer kan avsløre den ekte IP-adressen din under en aktiv VPN-økt.

- ○ Sant
- ○ Usant

9 Spørsmål 9

9. Med en VPN slått på og uten lekkasjer kan ikke internettleverandøren din se hvilke nettsteder du besøker.

- ○ Sant
- ○ Usant

10 Spørsmål 10

10. Å skjule IP-adressen din blokkerer sporing via nettleserfingeravtrykk.

- ○ Sant
- ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. En sikker tunnelomgåelse som avslører domeneforespørslene dine, kalles en _____ .

2. Nettleserbaserte _____ -kommunikasjons-API-er kan ved et uhell lekke din opprinnelige IP-adresse.

3. En _____ omdirigerer nettlesertrafikk, men krypterer ikke datapakkenes innhold.

4. Den flerlagde krypteringen i _____ -nettverket gir høy grad av anonymitet.

5. Din offentlige _____ tildeles av teleleverandøren din og avslører hvilket område du befinner deg i.

6. Å omgå regionale mediesperrer skjer ved maskering av _____ .

ORDBANK

DNS-LEKKASJE IP-ADRESSE MASKERING PLASSERING TOR VPN-TUNNEL WEBPROXY WEBRTC

Skriv svarene dine her:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Koble nettverksbegreper

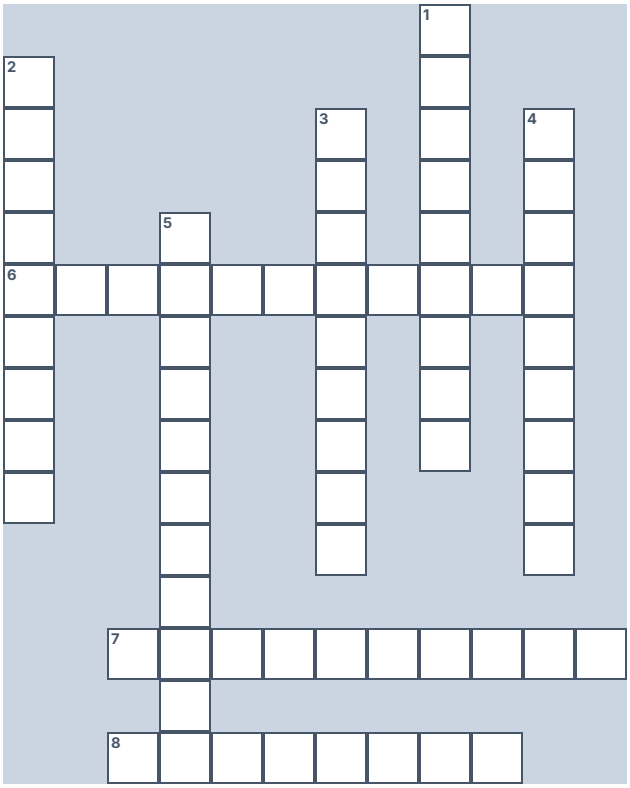
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. IP-adresse	A	Krypterer all trafikk fra en enhet og ruter den gjennom en VPN-server.
☐	2. VPN-tunnel	B	Sender data gjennom tre frivillige servere og krypterer lag for lag i hvert trinn.
☐	3. Tor-nettverket	C	Ruting av tilkoblingen gjennom en server i et annet land for å omgå geoblokkering.
☐	4. Webproxy	D	Unik numerisk etikett som identifiserer et enhetsgrensesnitt på internett.
☐	5. DNS-lekkasje	E	Omdirigerer nettlesertrafikk på applikasjonslaget uten systemkryptering.
☐	6. WebRTC API	F	Loggføringen av destinasjoner for ukryptert internettrafikk hos teleoperatøren din.
☐	7. Skjuling av posisjon	G	Spørringer som løses utenfor VPN-tunnelen og avslører besøkte domener for internettleverandøren.
☐	8. Sporing fra internettleverandøren	H	Nettleserfunksjon for tale/video som kan omgå tunneler og avsløre ekte IP-adresser.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

6. Ruter data gjennom tre frivillige servere og krypterer lag for lag i hvert trinn (11)

7. Logging av destinasjoner for ukryptert internettrafikk hos teleoperatøren din (10)

8. Omdirigerer nettlesertrafikk på applikasjonslaget uten kryptering på systemnivå (8)

LODDRETT

1. Unik numerisk etikett som identifiserer et enhetsgrensesnitt på internett (9)

2. Nettleserfunksjon for tale og video som kan omgå tunneler og eksponere reelle IP-adresser (9)

3. Krypterer all trafikk fra en enhet og ruter den gjennom en VPN-server (9)

4. Ruting av tilkoblingen gjennom en server i et annet land for å omgå geoblokkering (9)

5. Forespørsler som løses utenfor VPN-tunnelen og eksponerer besøkte domener for internettleverandøren (11)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

6 vannrett: Ruter data gjennom tre frivillige servere og krypterer lag for lag i hvert trinn (11 bokstaver):

7 vannrett: Logging av destinasjoner for ukryptert internettrafikk hos teleoperatøren din (10 bokstaver):

8 vannrett: Omdirigerer nettlesertrafikk på applikasjonslaget uten kryptering på systemnivå (8 bokstaver):

LODDRETT

1 loddrett: Unik numerisk etikett som identifiserer et enhetsgrensesnitt på internett (9 bokstaver):

2 loddrett: Nettleserfunksjon for tale og video som kan omgå tunneler og eksponere reelle IP-adresser (9 bokstaver):

3 loddrett: Krypterer all trafikk fra en enhet og ruter den gjennom en VPN-server (9 bokstaver):

4 loddrett: Ruting av tilkoblingen gjennom en server i et annet land for å omgå geoblokkering (9 bokstaver):

5 loddrett: Forespørsler som løses utenfor VPN-tunnelen og eksponerer besøkte domener for internettleverandøren (11 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

C G Å Y G L I V Å D O E S Z R
E N C W B A Å P P E W M A E Q
J I E F H J D N T S E N F J U
S R Å U G S Y T F A B A S Q O
A E R W Æ T S U L T R W U I D
K K O Ø B O G N U Z T Z K S A
K S T Å Ø R Ø N I M C H J P O
E A T L N N N E P V A Q Y S I
L M S S H E Å L A A P Q X P X
S G X C Ø T T Ø D B I I O O N
N Å H K P T R P R Z C N R R Å
D Ø G Æ Q V Y X E M X R P I B
P Y V N H E X D S Ø X L B N T
B Z Å Æ N R T S S Æ J Q E G E
A D L S Y K Z Z E M K I W W I

ORDLISTE

IPADRESSE VPNTUNNEL TORNETTVERK WEBPROXY DNSLEKKASJE
WEBRTCAPI MASKERING ISPSPORING

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. IPADRESSE
B. VPNTUNNEL
C. TORNETTVERK
D. WEBPROXY
E. DNSLEKKASJE
F. WEBRTCAPI
G. MASKERING
H. ISPSPORING

	DEFINISJONER OG TILHØRENDE FELT
	1. Omdirigerer nettlesertrafikk på applikasjonslaget uten kryptering på systemnivå.
	2. Ruting av tilkoblingen gjennom en server i et annet land for å omgå geoblokkering.
	3. Nettleserfunksjon for tale og video som kan omgå tunneler og eksponere reelle IP-adresser.
	4. Unik numerisk etikett som identifiserer et enhetsgrensesnitt på internett.
	5. Ruter data gjennom tre frivillige servere og krypterer lag for lag i hvert trinn.
	6. Logging av destinasjoner for ukryptert internettrafikk hos teleoperatøren din.
	7. Forespørsler som løses utenfor VPN-tunnelen og eksponerer besøkte domener for internettleverandøren.
	8. Krypterer all trafikk fra en enhet og ruter den gjennom en VPN-server.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale VPN-begreper. Skriv svarene dine i de utfyllbare svarboksene.

1. ERDPISSEA
2. EKOTRTREVTN
3. DKKASNJEESL
4. EGNKIRMAS
5. NUPLNTVEN
6. XYPOWREB
7. CWPIARETB
8. NSOGIPSRIP

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Grunner til å bruke en VPN på reise			
2	Nettlesere du kjenner til			
3	Ting en VPN kan skjule			
4	Ord knyttet til personvern			
5	Ord fra dette arbeidsarket du vil huske			
6	Ting et nettsted kan gjette ut fra IP-adressen din			
7	Tall eller symboler i en IP-adresse			
8	Myter om VPN-er			
9	VPN-tjenester du kjenner til			
10	Ting internettleverandøren din kan se			
11	Løfter en god VPN-leverandør gir			
12	Ting som kan lekke den virkelige IP-adressen din			
13	Grunner til å skjule posisjonen din			
14	Måter å skjule IP-adressen din på			
15	Enheter som kan bruke en VPN			

Kontrollpunkt 8: Casestudier om VPN

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

SARAH (STUDENT PÅ KAFÉ)

👷 «Hei! Jeg sitter på Coffee & Bytes. Der er det et usikret offentlig nettverk som heter «Free_Wi-Fi_No_Password». Jeg vil logge inn på skole-e-posten min og levere oppgaven min, men jeg er bekymret for hackere. Hva er risikoen ved å bruke dette nettverket uten en VPN, og hvordan sikrer en VPN dataene mine?»

ALEX (REISENDE STUDENT)

👷 «Å nei! Jeg reiser i utlandet i forbindelse med et prosjekt og prøver å se en biologidokumentar som ligger på en server i hjemlandet mitt. Men nettstedet sier «Denne videoen er ikke tilgjengelig der du befinner deg nå.» Hvorfor er jeg blokkert, og hvordan kan en VPN hjelpe meg å se den?»

Kontrollpunkt 9: Knekk chifferet

For å fullføre treningen i IP-maskering må du dekryptere denne hemmelige meldingen om å skjule de digitale sporene dine.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Æ=27 Ø=28 Å=29

19	11	10	21	12		1	4	18	5	19	19	5	14		4	9	14
13	5	4		5	20		19	11	10	21	12	20		19	25	19	20	5	13

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del A)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q1: Hva er en VPN, og hvordan fungerer den?

Et virtuelt privat nettverk (VPN) krypterer internettforbindelsen din og ruter trafikken gjennom en sikker ekstern server. Dette maskerer den offentlige IP-adressen din og begrenser hva observatører på lokale nettverk og internettleverandøren din kan se om trafikk som rutes gjennom VPN-tunnelen.

Q2: Hvorfor bør jeg bruke en VPN?

En VPN beskytter ditt digitale personvern, sikrer tilkoblingen din på offentlige Wi-Fi-nettverk (som kafeer eller flyplasser), kan redusere aktivitetsbasert struping når internettleverandøren ikke kan identifisere typen kryptert trafikk, omgår geografiske begrensninger for å få tilgang til globalt innhold og bidrar til å sikre ressurser for fjernarbeid.

Q3: Gjør en VPN meg helt anonym på nett?

Nei. Selv om en VPN skjuler IP-adressen din og krypterer trafikk, kan du fortsatt spores via informasjonskapsler i nettleseren, aktive kontoer (som Google eller Facebook), nettleserens fingeravtrykk eller hvis VPN-leverandøren din logger dataene dine.

Q4: Skjuler en nettproxy IP-adressen min?

Ja, men bare for trafikk som sendes gjennom den, vanligvis nettleseren din. De fleste webproxyer krypterer ikke dataene dine, så internettleverandøren din eller nettverksoperatøren kan fortsatt se hva du sender og mottar.

Q5: Er det lovlig å skjule IP-adressen min?

I mange land, ja, men noen begrenser eller forbyr VPN-er og andre verktøy som brukes til å skjule en IP-adresse. Å skjule IP-adressen din gjør aldri en ulovlig handling lovlig, så sjekk lokale lover før du bruker en.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om VPN (Del B)

Gå gjennom de vanligste spørsmålene og svarene potensielle kunder har om bruk av virtuelle private nettverk.

Q6: Skjuler Tor IP-adressen min?

Ja. Tor sender trafikken din gjennom tre frivillige relays (guard, middle og exit), slik at nettsteder ser adressen til exit-relayet, og ingen enkelt relay vet både hvem du er og hvor du går. [1]

Q7: Hva avslører IP-adressen min?

Den offentlige IP-adressen din avslører vanligvis internettleverandøren din og en omtrentlig plassering, for eksempel landet eller byen din. Nettsteder kan også bruke den til å knytte besøkene dine sammen og til å bruke geografiske sperrer.

Q8: Hvordan sjekker jeg at den er skjult?

Koble til VPN-en din, besøk deretter et nettsted for IP-kontroll og kjør DNS- og WebRTC-lekkasjetester. IP-adressen og DNS-serverne som vises, skal tilhøre VPN-en, ikke internettleverandøren din. Hvis din virkelige IP-adresse vises, slå på lekkasjebeskyttelse.

Q9: Kan jeg bruke en VPN på telefonen og smart-TV-en min?

Ja. Moderne VPN-leverandører tilbyr egne apper for iOS, Android, macOS, Windows, Linux og smart-TV-er, i tillegg til ruteroppsett som beskytter alle enhetene i hjemmenettverket ditt.

Q10: Hva er en Kill Switch?

En kill switch er en sikkerhetsfunksjon som automatisk kobler enheten din fra internett hvis VPN-tilkoblingen faller ut. Dette hindrer at ukrypterte data eller den virkelige IP-adressen din lekker ut.

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del C)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q1: Hvorfor kan nettsteder fortsatt spore meg etter at jeg har skjult IP-adressen min?

Å skjule IP-adressen din stopper ikke nettleserfingeravtrykk. Sporere kan kombinere detaljer som skjermoppløsning, installerte skrifttyper og nettleserinnstillinger til en identifikator, og informasjonskapsler eller innloggede kontoer kan også identifisere deg, så bruk også en personvernorientert nettleser. [3]

Q2: Hva er dobbel VPN eller Multi-Hop-ruting?

Multi-hop ruter trafikken din gjennom to eller flere VPN-servere i rekkefølge. Dette gir et ekstra lag med kryptering og bidrar til å holde den virkelige IP-adressen din skjult for den andre serveren hvis én server blir kompromittert.

Q3: Hva er WebRTC-lekkasje, og hvordan forhindrer en VPN den?

WebRTC er en nettleserprotokoll som kan avsløre dine ekte lokale og offentlige IP-adresser selv når et VPN er aktivt. Premium VPN-er blokkerer eller forfalsker WebRTC-forespørsler i appene for skrivebord og mobil og i nettleserutvidelsene sine.

Q4: Kan IPv6-trafikk avsløre min virkelige IP-adresse?

Ja, hvis VPN-en din bare tunnelerer IPv4. Enheten din kan da sende IPv6-trafikk utenfor tunnelen og avsløre en adresse som er tildelt av internettleverandøren din. Bruk en VPN som tunnelerer eller blokkerer IPv6, og bekreft det med en IPv6-lekkasjetest.

Q5: Hvordan omgår obfuskering VPN-blokkeringer?

Obfuskering (eller «Stealth VPN») skjuler VPN-trafikkpakker slik at de ser ut som vanlig HTTPS-nettrafikk (port 443). Dette bidrar til å komme forbi dyp pakkeinspeksjon (DPI), som myndigheter eller skole- og kontornettverk bruker for å blokkere VPN.

Kontrollpunkt 10: Avanserte vanlige spørsmål om VPN (Del D)

Utforsk tekniske og strukturelle sider ved virtuelle private nettverk og sikre tunnelprotokoller.

Q6: Avslører split tunneling min virkelige IP-adresse?

Ja, for appene du ekskluderer. Trafikk som sendes utenfor tunnelen bruker den virkelige IP-adressen din, og RFC 8828 påpeker at WebRTC kan avsløre internettleverandørens adresse under en VPN med delt tunnel, med mindre nettleseren begrenser det. [2]

Q7: Hva er en delt IP-adresse, og hvordan hjelper den personvernet?

Med delt IP framstår mange VPN-brukere online med samme adresse samtidig. Det gjør det mye vanskeligere for et nettsted å knytte ett enkelt besøk til deg enn med en dedikert IP som bare du bruker.

Q8: Kan internettleverandøren min se at jeg bruker en VPN for å skjule IP-adressen min?

Vanligvis ja. Internettleverandøren din kan se at du kobler til IP-adressen til en VPN-server, når du kobler til og hvor mye data du sender, men ikke nettstedene du besøker eller innholdet inne i den krypterte tunnelen.

Q9: Hva er beskyttelse mot DNS-lekkasjer?

DNS-lekkasjebeskyttelse tvinger enheten din til å sende oppslagsforespørsler for nettsteder (DNS-forespørsler) gjennom VPN-ens private, krypterte DNS-servere i stedet for internettleverandørens servere. Dette hindrer internettleverandøren din i å spore hvilke nettsteder du besøker.

Q10: Er en proxy eller en VPN best for å skjule IP-adressen min?

En VPN er vanligvis bedre. Den skjuler IP-adressen din for alle apper på enheten og krypterer trafikken, mens en nettproxy vanligvis bare dekker nettleseren og ofte ikke legger til noen kryptering.

Del 11: 10 interessante fakta om VPN og innsikt fra virkeligheten

Gå gjennom disse verdifulle, virkelighetsnære fakta og innsiktene om historien, markedet og teknologien bak VPN-er.

1. FØRSTE VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol), en tidlig VPN-protokoll fra en Microsoft-ledet gruppe på 1990-tallet, regnes nå som usikker, så moderne VPN-er bruker WireGuard eller OpenVPN.

2. FINGERAVTRYKK

Å skjule IP-adressen din stopper ikke nettleserfingeravtrykk, som kan identifisere deg ut fra detaljer som skjermoppløsning og installerte skrifttyper. [3]

3. WIREGUARD-REVOLUSJONEN

WireGuard har en svært strømlinjeformet kodebase som er utformet for effektivitet, noe som gjør det enklere å gjennomgå for sikkerhetssårbarheter enn tradisjonelle protokoller.

4. EKSPONERING AV WEBRTC-ADRESSE

RFC 8828 advarer om at WebRTC kan oppdage både en VPNs offentlige adresse og adressen til internettleverandøren som VPN-en kjører over, med mindre nettleseren begrenser det. [2]

5. OPPRINNELSEN TIL 5 EYES-ALLIANSEN

Etterretningspartnerskapet Five Eyes mellom USA, Storbritannia, Canada, Australia og New Zealand vokste ut av alliertes samarbeid om signaletterretning under andre verdenskrig.

6. DYP PAKKEINSPEKSJON

Avanserte brannmurer bruker Deep Packet Inspection (DPI) for å analysere metadata i nettverkspakker og blokkere typiske kjennetegn ved VPN-tilkoblinger.

7. GJENBRUK AV TOR-KRETS

Tor gjenbruker den samme kretsen i omtrent ti minutter og bygger deretter en ny, noe som gjør det vanskeligere å koble sammen nettaktiviteten din. [1]

8. DESENTRALISERTE VPN-ER

Desentraliserte VPN-er (dVPN-er) fordeler trafikken over et nettverk av noder drevet av likemenn (peers), noe som reduserer avhengigheten av én enkelt sentralisert leverandør.

9. ANONYMITET MED TOR MOT VPN

En VPN tunnelerer trafikk gjennom én enkelt leverandør, mens Tor (The Onion Router) sender trafikk gjennom tre frivillige reléer (inngang, mellomledd, utgang) for å maksimere personvernet. [1]

10. PROXYER MOT VPN-TUNNELER

En nettproxy endrer IP-adressen et nettsted ser for nettlesertrafikken din, men i motsetning til en VPN krypterer den vanligvis ikke trafikken og dekker ikke andre apper på enheten din. [5]

Tekniske referanser og kilder

Siterte publikasjoner, kryptografiske spesifikasjoner og offisielle dokumentstandarder som er brukt i dette arbeidsarket.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Fasit: Skjuling av IP-adresser, stedsmaskering, proxy, Tor og forebygging av DNS-/WebRTC-lekkasjer

1 **Spørsmål 1** **Riktig svar: B**

MERKNAD TIL LÆREREN

Hva avslører en enhets offentlige IP-adresse for nettstedene du besøker? → Din omtrentlige plassering og navnet på internettleverandøren din

2 **VPN-systemkryptering** LATENS **Riktig svar: C**

MERKNAD TIL LÆREREN

I motsetning til proxyer som bare omdirigerer nettlesertrafikk, oppretter en VPN en kryptert tunnel for hele systemet og sikrer bakgrunnsapplikasjoner, spill og spørringer fra operativsystemet.

3 **Manglende kryptering i proxyer** WI-FI-SIKKERHET **Riktig svar: A**

MERKNAD TIL LÆREREN

Webproxyer videresender bare nettlesertrafikk uten å kryptere pakkenes innhold, noe som betyr at nettverksoperatøren eller internettleverandøren din fortsatt kan spore innholdstrafikken din.

4 **Spørsmål 4** **Riktig svar: B**

MERKNAD TIL LÆREREN

Hvordan gir Tor-nettverket brukerne høy anonymitet? → Ved å rute trafikken gjennom tre reléer drevet av frivillige

5 **DNS-tunnellekkasjer** PERSONVERN **Riktig svar: B**

MERKNAD TIL LÆREREN

En DNS-lekkasje oppstår når forespørsler om domenenavnoppslag omgår VPN-tunnelen og går direkte til internettleverandørens oppløsere, slik at oppføringer om besøkte domener eksponeres.

Fasit: Kontrollpunkt 2 – sant eller usant

6 Detaljer om proxyens begrensninger

IP-MASKERING

Riktig svar: Usant

MERKNAD TIL LÆREREN

Proxyer fungerer på applikasjonslaget og mangler den systemomfattende integreringen av nettverksdrivere som en VPN-tunnel har.

7 Spørsmål 7

Riktig svar: Sant

MERKNAD TIL LÆREREN

Å videresende trafikk gjennom tre reléer drevet av frivillige med lagdelt kryptering gir økt forsinkelse, så Tor er vanligvis tregere enn en direkte tilkobling.

8 Spørsmål 8

Riktig svar: Sant

MERKNAD TIL LÆREREN

WebRTC kan avsløre lokale adresser og, med enkelte VPN-oppsett, den offentlige IP-adressen internettleverandøren har tildelt, under tunnelen (RFC 8828).

9 Spørsmål 9

Riktig svar: Sant

MERKNAD TIL LÆREREN

Uten DNS- eller WebRTC-lekkasjer ser internettleverandøren bare kryptert trafikk til VPN-serveren, ikke nettstedene du besøker.

10 Begrensninger ved fingeravtrykk

INGEN LOGGING

Riktig svar: Usant

MERKNAD TIL LÆREREN

Fingeravtrykk (fingerprinting) retter seg mot måleverdier for enhetens konfigurasjon (skjermoppløsning, skrifttyper, programtillegg) som forblir synlige selv når IP-adressen er skjult.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

D 1. IP-adresse	A 2. VPN-tunnel	B 3. Tor-nettverket	E 4. Webproxy
G 5. DNS-lekkasje	H 6. WebRTC API	C 7. Skjuling av posisjon	F 8. Sporing fra internettleverandøren

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 DNS-LEKKASJE	2 WEBRTC	3 WEBPROXY	4 TOR
5 IP-ADRESSE	6 PLASSERING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 D – WEBPROXY	2 G – MASKERING	3 F – WEBRTCAPI	4 A – IPADRESSE
5 C – TORNETTVERK	6 H – ISPSPORING	7 E – DNSLEKKASJE	8 B – VPNTUNNEL

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare IP-adresse, VPN-tunnel og Tor-nettverket med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

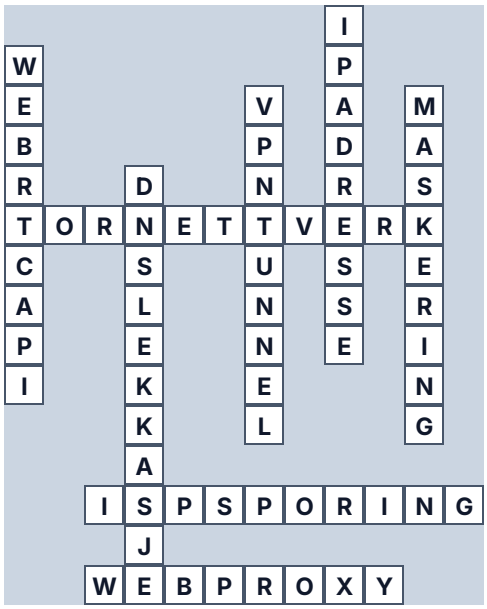
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

C	G	Å	Y	G	L	I	V	Å	D	O	E	S	Z	R
E	N	C	W	B	A	Å	P	P	E	W	M	A	E	Q
J	I	E	F	H	J	D	N	T	S	E	N	F	J	U
S	R	Å	U	G	S	Y	T	F	A	B	A	S	Q	O
A	E	R	W	Æ	T	S	U	L	T	R	W	U	I	D
K	K	O	Ø	B	O	G	N	U	Z	T	Z	K	S	A
K	S	T	Å	Ø	R	Ø	N	I	M	C	H	J	P	O
E	A	T	L	N	N	N	E	P	V	A	Q	Y	S	I
L	M	S	S	H	E	Å	L	A	A	P	Q	X	P	X
S	G	X	C	Ø	T	T	Ø	D	B	I	I	O	O	N
N	Å	H	K	P	T	R	P	R	Z	C	N	R	R	Å
D	Ø	G	Æ	Q	V	Y	X	E	M	X	R	P	I	B
P	Y	V	N	H	E	X	D	S	Ø	X	L	B	N	T
B	Z	Å	Æ	N	R	T	S	S	Æ	J	Q	E	G	E
A	D	L	S	Y	K	Z	Z	E	M	K	I	W	W	I

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

6 vannrett: TORNETTVERK Ruter data gjennom tre frivillige servere og krypterer lag for lag i hvert trinn (11 bokstaver)

7 vannrett: ISPSPORING Logging av destinasjoner for ukryptert internettrafikk hos teleoperatøren din (10 bokstaver)

8 vannrett: WEBPROXY Omdirigerer nettlesertrafikk på applikasjonslaget uten kryptering på systemnivå (8 bokstaver)

LODDRETT

1 loddrett: IPADRESSE Unik numerisk etikett som identifiserer et enhetsgrensesnitt på internett (9 bokstaver)

2 loddrett: WEBRTCAPI Nettleserfunksjon for tale og video som kan omgå tunneler og eksponere reelle IP-adresser (9 bokstaver)

3 loddrett: VPNTUNNEL Krypterer all trafikk fra en enhet og ruter den gjennom en VPN-server (9 bokstaver)

4 loddrett: MASKERING Ruting av tilkoblingen gjennom en server i et annet land for å omgå geoblokkering (9 bokstaver)

5 loddrett: DNSLEKKASJE Forespørsler som løses utenfor VPN-tunnelen og eksponerer besøkte domener for internettleverandøren (11 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. E R D P I S S E A — **IPADRESSE**
2. E K O T R T R E V T N — **TORNETTVERK**
3. D K K A S N J E E S L — **DNSLEKKASJE**
4. E G N K I R M A S — **MASKERING**
5. N U P L N T V E N — **VPNTUNNEL**
6. X Y P O W R E B — **WEBPROXY**
7. C W P I A R E T B — **WEBRTCAPI**
8. N S O G I P S R I P — **ISPSPORING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"SKJUL ADRESSEN DIN MED ET SKJULT SYSTEM"

Fasit til casestudiene

A Scenario A: Sikkerhet på offentlige nettverk

SNIFFING OG KRYPTERING | Sarahs dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Risikoer: Pakkesniffing, avlytting av data og man-in-the-middle-angrep. Noen på det samme nettverket på kafeen kan fange opp innloggingsopplysningene hennes eller lekse-filen hennes.
- VPN-beskyttelse: Krypterer nyttelastene i nettverkspakkene, slik at avlyttet tunneltrafikk blir uleselig for passive snusere i det lokale nettverket når VPN-en er riktig konfigurert.

B Scenario B: Tilgang til blokkerte ressurser

GEOBLOKKERING OG IP-ADRESSER | Alex' dilemma

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Hvorfor blokkert: Strømmetjenesten bruker geoblokkering, som kobler reisendes lokale IP-adresse til hans fysiske land og blokkerer den basert på territoriell lisensiering.
- Slik hjelper VPN: Han maskerer sin virkelige posisjon ved å rute trafikken gjennom en server i hjemlandet sitt. Nettstedet ser en IP-adresse fra hjemlandet, og han får tilgang.